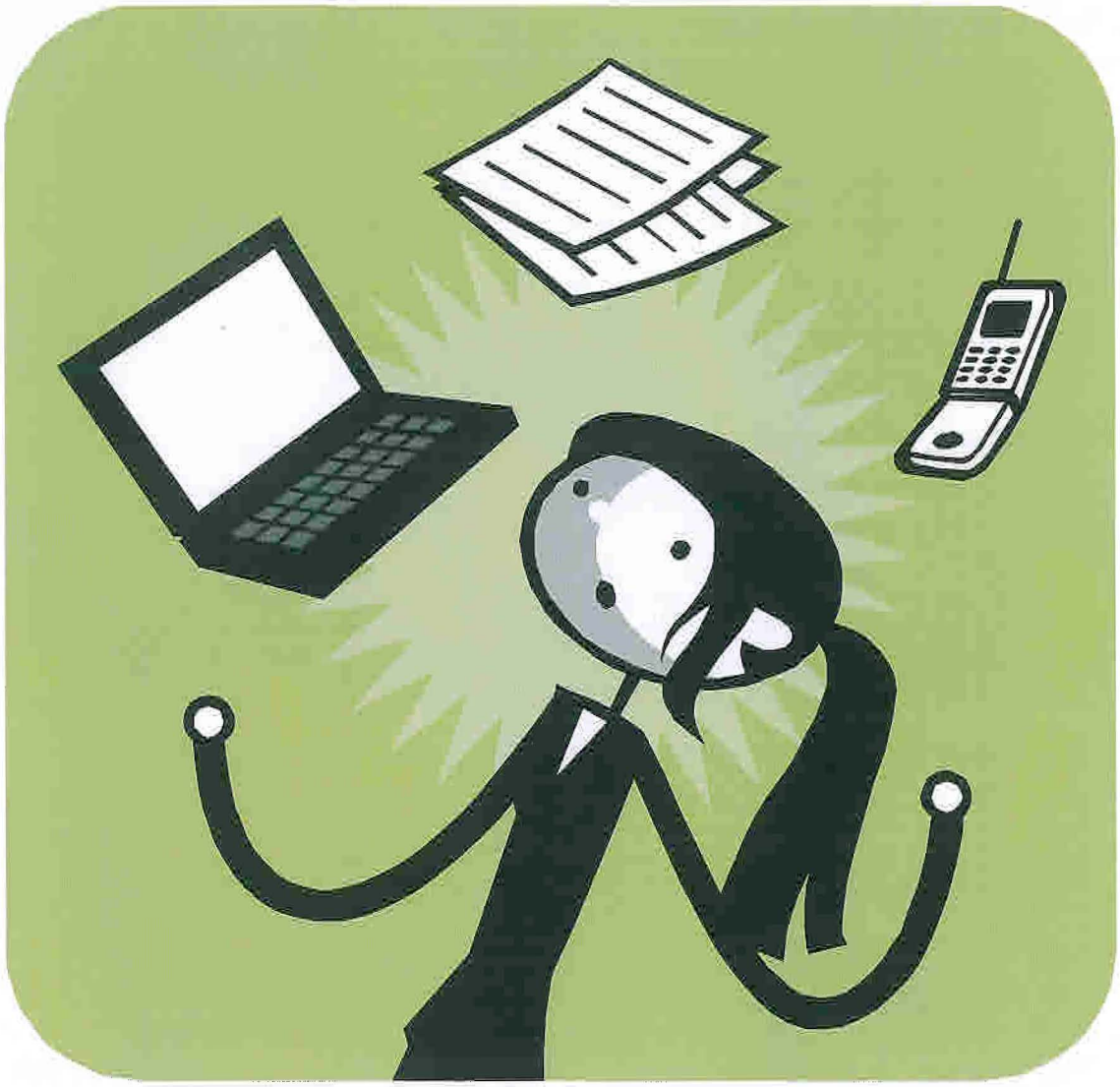
IT Policies



USDA

APR 1 8 2011

United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue SW

Washington, DC 20250

TO: Agency Administrators
Agency Deputy Administrators for Management
Departmental Management
Agency Chief Information Officers
Information Systems Security Program Managers

FROM: Charles T. McClam
Deputy Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Minimum Safeguards for Protecting Personally Identifiable Information

USDA in the fulfillment of its mission collects, maintains, and processes vast amounts of sensitive and personally identifiable information (PII). As such, each USDA employee, contractor, affiliate, and partner has a vital role in protecting all personally identifiable and sensitive information entrusted to them. All USDA employees, contractors, partners and affiliates must exercise extreme care in the handling of PII. Failure to properly protect and control PII may result in disciplinary actions, in accordance with USDA policies.

The Office of Management and Budget (OMB) established guidance for protecting PII in memoranda M-06-15, *"Safeguarding Personally Identifiable Information" and M-06-16, "Protection of Sensitive Agency Information."* In these memos, the OMB defines PII as "any combination of information about an individual maintained by the agency, including but not limited to name, social security number, date of birth, maiden name, biometric record number, home address, education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity."

In addition to OMB's memoranda, the Office of the Chief Information Officer (OCIO) issued multiple memoranda on protecting and safeguarding paper based, and electronic PII. USDA employee, contractors, affiliates, and partners are reminded that the removal PII (either paper based or electronic) from the workplace without prior written authorization from the USDA unit manager or other authorized senior agency official is prohibited.

Paper based PII
Paper-based PII incidents can be reduced by securing all PII in an approved locked storage container or device when not in use, and adhering to the Department's physical transport of PII guidance (attached).

Mobile Media Storage Devices
Extreme care must be exercised in the storage, transport, and usage of mobile media devices containing PII. Mobile media devices include, but are not limited to; compact disk (CD), digital video device (DVD) and universal serial bus (USB).

Individuals who use CDs and DVDs to process PII, must encrypt and password protect the file containing the PII, and transport the media device and the password separately. USB devices used by USDA employees, contractors, and affiliates to process or store PII must be Government issued encrypted USBs devices. The processing and storage of PII and sensitive information on a personal and/or unencrypted USB is strictly prohibited.

Password Protection
Use a complex password for files containing PII which are being stored or transmitted. The password complexity should contain upper and lower case letters, numbers, and special character. The password should be transmitted separately from the file.

Reporting a PII Incident
Immediately report PII incidents to the PII hot line at 1-877-PII-2-YOU, or 1-877-744-2968. The hotline is operational twenty-four hours a day seven days a week.

PII Requirements Assistance
USDA employees, contractors, and affiliates should consult their agency Information Systems Security Program Manager, Agency Privacy Official, or agency Chief Information Security Officer for assistance in satisfying the above requirements.

If you have any questions regarding this memorandum, please contact Ms. Ray Payton, Chief Privacy Officer at (202) 720-8755 or ray.payton@ocio.usda.gov.

Attachment
Personally Identifiable Information (PII) Physical Transport – Double Wrap Procedures

Personal Identifiable Information (PII) Physical Transport—Double Wrap Procedures

Instructions:

USDA processes all types of sensitive information and it is essential that this information be properly handled and protected. PII is considered Sensitive But Unclassified (SBU) Information. Careless handling and transporting PII information puts USDA at risk.

USDA policy prescribes specific procedures for the transport of PII. When Physical Transport is necessary:

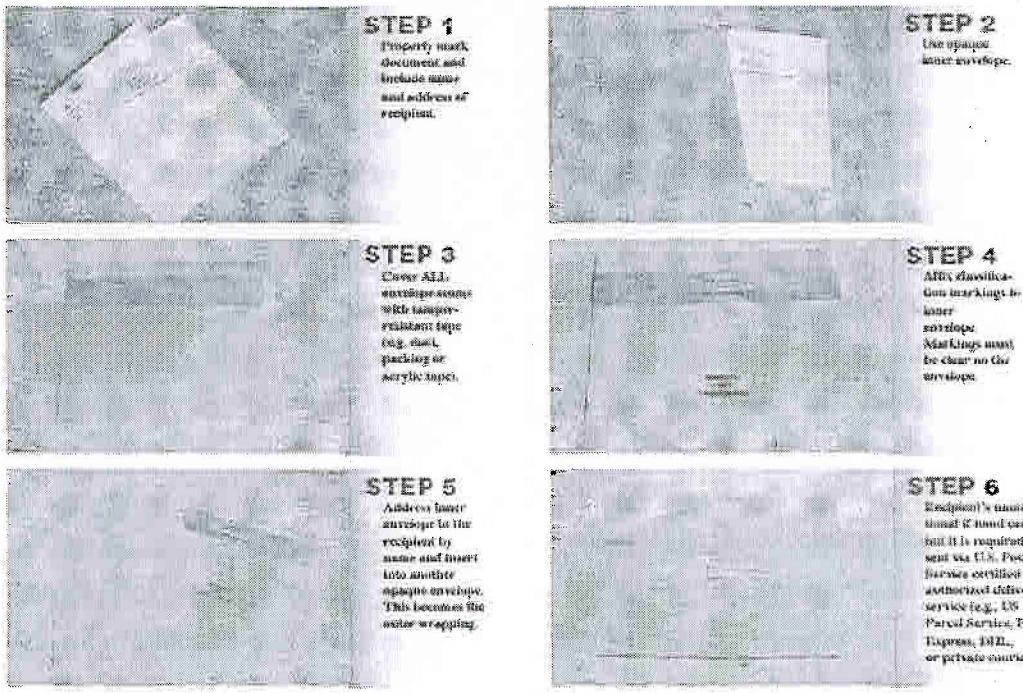
1. Encrypt portable media containing PII
2. Use NIST approved encryption method
3. Double wrap portable media
4. Transport by Postal Service or another authorized delivery service
5. Transmit decryption key separately via certified mail
6. Mark physical documents containing PII: "Sensitive But Unclassified / Sensitive Security Information—Disseminate on a Need-to-Know Basis Only"
7. Documents should be double wrapped
8. Transport by Postal Service or another authorized delivery service

Portable media should be double-wrapped in an opaque package or container that is sealed sufficiently to prevent inadvertent opening and to show signs of tampering. The package must be sent via a certified carrier with an ability to track pickup, receipt, transfer, and delivery.

Portable media may be transmitted by interoffice mail or briefcase provided it is double-wrapped to afford sufficient protection against inadvertent or unauthorized access.

Please follow the instructions below when transporting PII information. The steps listed on the chart, must be followed with no exceptions. If you have any questions or concerns, please contact us at cyber.incidents@asoc.usda.gov or 1-866-905-6890.

"Protect It Like Your Own"



USDA

United States Department of Agriculture

NPARL Network Security and Best Practices Policy

Purpose: This agreement establishes policies to ensure comprehensive protections are in place to safeguard all information technology resources of the U.S. Government and NPARL. For violation of any policies, disciplinary action will be taken at the discretion of ARS management.

As a user of USDA/ARS/NPARL computer equipment, I agree to:

- **Use good password management, which involves the following:**
  - Use passwords that contain a **minimum of 8 characters** and keep them confidential. (This includes passwords for network access as well as E-mail accounts.
  - Do not choose anything that is easily guessed or is associated with you. Examples of this would include dictionary words, your name, your name spelled backwards, your dog's name, a nickname, a favorite team, a hobby, your license plate number, a blank password or the word "password".
  - Use a combination of letters, numbers, and symbols to construct your password to make the password more secure.
  - Change your passwords **a minimum of every 90 days**. Your network login password will automatically expire every 90 days and will require you to change it. However, your GroupWise email password does not expire, and it is up to you to change this password and make sure it follows the password rules that are listed above.
  - It is strongly recommended that you **do not write down your password**. If you use several systems which require password access and thus have too many passwords to remember, and you find that you must record them somewhere, make sure they are kept in a secure location (i.e., in an encrypted file on your PC, locked in a file cabinet, or in your wallet). Never post your passwords under your keyboard, on your monitor, in an unlocked desk drawer, or any other easy to find location
  - Do not share the password to your office PC with anyone; including your supervisor, co-workers, or Information Technology (IT) support staff. Files, databases, or systems which must be shared among several authorized users should be maintained on a network or shared drive. Passwords to shared PCs should only be shared among authorized users.
    - If your IT support staff needs access to your system, he/she should request that you enter the password yourself. If this is impractical, you should change it immediately upon the completion of the service work.
    - If it is necessary to share your password with your supervisor or co-worker for an emergency or critical purpose while your are out of the office, change your password immediately upon returning to the office.

- **Use my own individual user name and password when connecting to network resources**

- **Be accountable for my actions on my individual computers and network resources**

- **The monitoring of all computer usage and network related activities that take place on the local area network.**

- **NOT make illegal copies of software or install software on multiple machines when the license does not grant such permission explicitly.**

Individual Users agree to: *(Continued)*

- **NOT install any software or hardware that is brought in from home.**

- **NOT install any software that is downloaded from the Internet without first checking with the IT Support Staff to make sure that the software is legitimate and free from malicious or harmful code.**

- **NOT bring in personal computer equipment to use for official business.**
  - If personal equipment is brought in and used and gets damaged, lost, or stolen, the government bears no responsibility for any losses.

- **NOT hook up any analog modems to my computer and/or attempt to connect to the Internet using a modem connection.**
  - Connecting to the Internet via modem bypasses all security provisions (firewalls, packet filters, antivirus, etc) that have been established and places the entire network at risk for intrusion.

- **NOT setup any type of wireless networking equipment at the Location. (Including, but not limited to, network cards, access points, routers, etc…)**

- **NOT access systems and/or applications, within the building, to which access has not been authorized.**

- **Check with the IT Support Staff before purchasing all computer related products, and only purchase those products (software and hardware) that have been approved by the IT Support Staff. This helps to alleviate compatibility issues and ensures that the Laboratory remains in compliance with government regulations.**

- **Obtain authorization from supervisor for the use of government computer equipment outside of the NPARL Location.**

- **Perform the following to help prevent Unauthorized System Access**
  - Log out of the network or lock your workstation if you plan to be away from your computer for any extended time (e.g., lunch, meeting, etc.).
  - Use a password protected screensaver which invokes within 10 minutes (or other suitable timeframe) of inactivity on your PC.
  - Turn off your computer if you are away from the office for an extended length of time.
  - Take appropriate steps to thoroughly clean hard drives before equipment is reassigned, surplused, or discarded. Consult with your IT support staff for steps to be taken.
  - Be sensitive to co-workers or other persons looking over your shoulder while using your PC.

Individual Users agree to: *(Continued)*

- **Perform the following to help prevent Loss of Critical Data**
  - Backup files and data resident on your individual PCs on a regular basis. (If you do not know how to back up your data, or don't realize the possible consequences of not backing up your data, consult with your IT support staff for guidance and assistance on recommended backup tools and methodology.)
  - Properly label media used for backing up files and maintain in a locked, and if possible, fire-proof or off-site location.
    - If you are in need of locked and fire-proof storage, your backup media can be given to your IT support staff, and it will be stored for you in our fire-safe vault.

- **Use the following provisions when Working at an Alternate Site**
  - All security measures discussed above should also be considered while working at home or a satellite work site.
  - If available, obtain certification from authorized officials at satellite work sites indicating that the site provides adequate protection for sensitive information and that such use conforms to applicable laws or policies.
  - Sensitive materials and information may only be stored at an alternate work site if they can be locked in a secure cabinet or drawer.
  - Government IT resources which have been installed at home may be used for authorized purposes only, and may only be used by the individual to whom it is assigned. No friends, family members, or other acquaintances are allowed to use government equipment at any time.
  - Use caution when exchanging files and disks between a home and office PC. These files and disks can contain viruses (especially if the home PC is also used by other family members) and should be scanned before use. Your office PC has an antivirus solution, and will automatically scan all disks that are inserted.

Individual Users agree to: *(Continued)*

- **Use the following provisions while in Travel Status and/or using your Laptop**
  - If you possess a laptop, keep it locked in a file cabinet or other secure area when not in use. When using your laptop, whether at the Location, at home, or on the road, use the Kensington laptop security device provided by the IT support staff to secure it to your desk or other stable object.
  - If you carry a laptop computer and/or Personal Digital Assistant (PDA) while traveling, keep it close at hand or locked in a secure location at all times.
  - Always carry your laptop and/or PDA with you while traveling by plane or other public transportation, and do NOT put your laptop or PDA in checked baggage.
  - When using a hotel Ethernet network connection to access the Internet, use it sparingly and don't let your computer remain connected for long periods of time. These "Always-On" connections are more vulnerable to computer attacks. In addition, extra security can be obtained by installing an application firewall on your laptop such as ZoneAlarm. Consult your IT Support Staff if you need help with this matter.
  - If you use a public computer (university computer lab, Internet café, friends house, etc…) to access your email via the web, be aware that you have no idea what programs could be running in the background. There are sniffers or keyboard loggers that could be running that can capture your every keystroke. So if you ever use these types of systems, it is a good idea to change your email password when you return to the Location.
  - If using your laptop or PDA for work while in transit, be sensitive to fellow travelers looking over your shoulder.

- **Abide by REE Policy 253.4, "Use of Information Technology Resources" at:** http://www.afm.ars.usda.gov/ppweb/253-4.htm

- **Abide by the Department Regulation 3140.2, USDA Internet Security Policy at:** http://www.reeusda.gov/issp/dr3140-1.htm

USDA

United States Department of Agriculture

Research, Education, and Economics
Agricultural Research Service

September 29, 2003

SUBJECT: Limited Personal Use Policy

TO: All ARS Employees

FROM: Melinda L. McClanahan /s/
Chief Information Officer

The Agricultural Research Service (ARS) Office of the Chief Information Officer reminds ARS employees and contractors that the U.S. Department of Agriculture (USDA) and ARS both have a "Limited Personal Use Policy" that cannot be used as a justification for illegal or inappropriate use and practices. All **ARS** contractors and consultants need to be advised that they are subject to compliance with all federal laws and USDA regulations when they and/or their company are receiving **ARS** funds for services they are performing on behalf of the Agency. Use of non-ARS, non-federal computers, including laptops, does not exempt the contractor from ARS and federal laws.

The following activities as outlined in Departmental Regulation 3300-1, "Telecommunications & Internet Services and Use," Appendix I and ARS Policy and Procedure 253.4 are unacceptable uses of information technology resources, specifically the use of the USDA Internet Access Network (IAN). Not only are these activities illegal, but they also clog networks, slow down use of the internet for legitimate business purposes, and open ARS networks to intrusion by outsiders.

- The creation, downloading, viewing, storage, or copying of sexually explicit or sexually oriented materials. (**All** instances of pornography will be forwarded to the Office of the Inspector General).

- The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, weapons, terrorist activities, and any other illegal or prohibited activities.

ars

Office of the Chief Information Officer
5601 Sunnyside Avenue • Beltsville, MD 20705-5119

- Posting Agency information to external news groups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained.

- Using government systems as a staging ground or platform to gain unauthorized access to other systems.

- Any use of peer-to-peer (P2P) software (e.g., KaZaA, Morpheus, eMule, etc.). P2P software is used for the illegal exchange of software, music, videos, and graphics that are protected by copyright laws. The unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by national and international copyright laws, trademarks, or other intellectual property rights are prohibited. (**Users** will be personally responsible for all costs related to trafficking in music, software, and videos if a complaint is filed against them and the copyright owner seeks restitution of funds lost due to pirating copyright protected material.)

- Personal use of Web Browser feature add-ons (e.g., Instant Messaging, Real Player, etc.) to listen to radio broadcasts or music for entertainment and Broadband tools (e.g., Shockwave, Window Media, Flash, etc.) that overburden the telecommunications system via an internet connection. (Web Browser feature add-ons used for Official Business such as on-line training courses are allowed.)

The USDA's Cyber Security office monitors all USDA Internet activities on a daily basis. Employees and contractors who are using the IAN for any of the activities described above will be detected via the Department's monitoring tools and will be subject to disciplinary action.

Disciplinary actions include appropriate administrative actions taken against employees/contractors violating this policy. This includes dismissal and referring computer misuse cases to the appropriate U. S. Attorney's office for possible criminal indictment.

If you have any questions or concerns regarding the above guidelines, please contact the ARS Information Systems Security Program Manager, Bill Keen at bkeen@ars.usda.gov.

Additions and Clarifications to ARS P&P 253.4

(5/21/2002)

Make sure you read ARS P&P 253.4 "Use of Information Technology Resources" before reading and signing the following document.

Section #2 - Unacceptable Personal Use

The following applications are also considered to be unacceptable to install or use at any time; unless special authorization has been granted.

- Streaming media programs such as Real Player, Windows Media Player, or others in which the function is to view Internet video or listen to Internet radio.
- Yahoo Messenger, MSN Messenger, AOL Instant Messenger or others in which the primary function is to send messages or chat with other people.
- Any program that provides Internet phone connectivity or allows people to communicate from their PC's to a telephone.
- Programs that allow the participation in any file sharing or file swapping activities. (Examples: Napster, Limewire, Morpheus, Kazaa, Gnutella, etc)

United States Department of Agriculture
Research, Education, and Economics

ARS ❑ CSREES ❑ ERS ❑ NASS

Policies and Procedures

Title: Use of Information Technology Resources

Number: 253.4

Date: April 19, 2002

Originating Office: Information Technology Division, AFM/ARS

This Replaces: P&P 253.4 dated September 3, 1999, and Bulletin 98-001 dated 3/20/98

Distribution: All REE Employees

This P&P defines acceptable and unacceptable uses of information technology (IT) resources such as telephones, E-mail, facsimile machines, cellular telephones and Internet services. **This was modified on July 8, 2002, to apply the same rules to cellular phones as are in place for land-line phones.**

Table of Contents

1. Introduction

Agencies provide REE employees with information technology (IT) resources (e.g., PCs, E-mail, telephones, facsimile machines, copiers, office equipment, Internet access, etc.) to support mission accomplishment and enhance the efficient and effective delivery of services to agency customers. This P&P describes appropriate use of these resources and establishes conditions under which employees may use IT resources for non-Government purposes.

2. General Policy

Introduction

IT resources may only be used for authorized purposes. However, "limited personal use of Government office equipment by employees during personal time is considered to be an 'authorized use' of Government property", according to Departmental Regulation (DR) 3300-1, dated March 23, 1999. In the REE agencies, "limited personal use" is use that involves minimal additional expense to the Government, is performed on the employee's personal time, and does not interfere with the mission or operations of an agency.

Employees are expected to abide by this and other rules and regulations and to be responsible for their own personal and professional conduct. The Standards of Ethical Conduct state "employees shall put forth honest effort in the performance of their duties" (Section 2635.101 (b)(5)).

Supervisors have the management authority and responsibility to ensure the appropriate use of resources within their organizations. This includes IT resources and official employee time. As such, employees should consult with their supervisors regarding authorized use of IT resources and interpretation of this P&P. The privilege to use Government office equipment for non-Government purposes may be revoked or limited at any time by supervisors or other appropriate agency officials.

It is encouraged to manage telecommunications services in accordance with DR 3300-1 (Telecommunications & Internet Services and Use), and other pertinent laws and regulations. DR 3300-1 can be found at URL: http://www.usda.gov/ocio/directives/DR/DR3300-001.htm

Personnel traveling (domestic and international) should review the Departmental Regulation 2300-003 (Authorized Telephone Calls of a Personal Nature During Official Travel), prior to traveling and claiming expenses. DR 2300-003 can be found at URL: http://www.usda.gov/ocio/directives/DR/DR2300-003.htm

Acceptable Personal Use

Employees are permitted limited use of Government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of Government office equipment should take place during the employee's personal time, such as before or after duty hours or lunch periods.

Personal use of Government office equipment is limited to situations where the Government is already providing equipment or services and the employee's use of them will result in only minimal additional expense to the Government. This would include normal wear and tear or the use of small amounts of electricity, ink, toner, or paper.

Unacceptable Personal Use

Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment for activities that are inappropriate. Unacceptable personal use of Government IT resources includes:

- Any use that could generate more than minimal additional expense to the Government.
- Any use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, the forwarding of "chain" e-mails, e-mailing greeting cards, or downloading of video, sound or other large file attachments can degrade the performance of the entire network.
- Activities that are illegal or offensive to fellow employees or the public. Examples include pornography, hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Any use for commercial purposes or "for-profit" activities such as outside employment or to support a personal private business activity (e.g., consulting for pay, sales, or administration of business transactions, sale of goods or services).
- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

3. Telephone Equipment and Services

Acceptable Personal Use

The use of Government telephone systems (including government issued cellular telephones and calls over commercial systems which will be paid for by the Government) are in place for the conduct of official business or limited personal use as outlined above in General Policy. Calls

may be made using Government-issued wireless phone service when policies outlined for land-line phones are followed. The use of cellular technology at the expense of the government does not preclude the user from having the responsibility for inventory control, billing and accountability.

Employees may make the following personal calls at Government expense:

- Brief daily calls to locations within the local commuting area to check the condition of your spouse or children.
- Calls to your family, your doctor, etc., if you are hurt on the job.
- Calls to advise your family and/or to make other transportation or child care arrangements if you must work overtime without advance notice.
- Calls to business offices open only during the work day.
- Calls to schedule emergency home or car repairs.
- Calls to your home once a day while on Government travel/business.
- Calls to your home while on Government travel/business to advise your family of travel changes or delays.

Employees may make personal calls **not** at Government expense if the call is:

- charged to your home phone number or other non-Government number;
- made to an 800, 877, 888, or other toll-free number;
- charged to the called party if a non-Government number (collect call); or
- charged to a personal credit card or prepaid calling card.

Unacceptable Personal Use

Unacceptable use includes:

- Making an unauthorized telephone call with the intent to later reimburse the Government.
- Use of "900" calls to include dialing a toll free number which will switch to a "900" call, either on or off the FTS2001/WorldCom network.

- Collect calls and third party calls charged to a Government number.

4. E-mail

Acceptable Personal Use

Acceptable E-mail messages include:

- Occasional personal messages.
- Inquiries about your salary, insurance, retirement, or other employee benefits.

Unacceptable Personal Use

Unacceptable uses of E-mail include:

- The creation, copying, or transmission of "junk mail" such as chain letters, hoaxes, advertisements, solicitations, or other unauthorized mass mailings.
- Spreading computer viruses warnings (hoaxes). While these hoaxes do not infect systems, they are time consuming and costly to handle. You should be especially alert if the warning urges you to pass it on to your friends. Forward these messages to your Information Systems Security Officer for evaluation.
- Engaging in any outside fund-raising activities.
- Sending large attachments that degrade system performance.

5. Internet

Acceptable Personal Use

Acceptable uses of the Internet during employee personal time include:

- Accessing the Employee Personal Page or the Thrift Savings Plan to check balances or make changes.
- Communicating with a volunteer charity organization.
- Looking at vacancy announcements.

- Collecting information for personal travel or other such personal activities.

Unacceptable Personal Use

Unacceptable uses of the Internet include:

- The creation, downloading, viewing, storage, or copying of sexually explicit or sexually oriented materials.

- The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, weapons, terrorist activities, and any other illegal or prohibited activities.

- Posting agency information to external news groups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained.

- Using Government systems as a staging ground or platform to gain unauthorized access to other systems.

- The unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by national and international copyright laws, trademarks, or other intellectual property rights.

- Participating in chat rooms.

6. Facsimile Machines, Copiers, and Printers

Acceptable Personal Use

Examples of acceptable use of facsimile machines, copiers, and printers include:

- Occasional use of fax calls to locations within the local commuting area. Fax calls outside the local commuting area are authorized only if not charged to the Government (see Telephone section).

- Making a few photocopies.

- Using a printer to print a few pages of material.

Unacceptable Personal Use

Unacceptable use of facsimile machines, copiers, and printers include:

- Making long distance fax calls at Government expense.

- Making more than a minimal amount of photocopies, making photocopies of illegal or offensive material, or making photocopies for commercial or "for-profit" purposes.

7. Sanctions for Misuse

Unauthorized or improper use of IT resources may result in loss or limitations on use of equipment or services, disciplinary action, criminal penalties, or financially liability for the costs of the use.

8. Privacy Expectations

Each agency has the responsibility to ensure that employees are not abusing the privileges offered by this policy. The policy does not change, in any way, the agency's right to inspect equipment when there is evidence or a strong suspicion that an employee is abusing this policy.

Employees do not have a right to, nor should they expect, privacy while using any Government office equipment at any time. To the extent that employees wish their private activities remain private, they should avoid using an agency's office equipment, such as their computer, the Internet, E-mail, photocopiers, or facsimile machines, or cellular or land-line phones, for their personal use. By using Government office equipment employees imply their consent to disclosing the contents of any files or information maintained or passed through Government office equipment. Any use of Government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

System managers do employ monitoring tools to detect improper usage. Electronic communications may be disclosed within an agency to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access any electronic communications.

SAFETY

Current Federal policy (GSA Bulletin FMR B-2, March 1, 2002) outlines policy for the use of cellular phones in motor vehicles. It is recommended while operating a Personal vehicle and/or Government vehicle, and you need to make or answer a telephone call that you safely pull the vehicle to the side of the road and bring the vehicle to a complete stop, until you have completed the telephone call. Some state and city laws prohibit the use of cellular telephones while operating a vehicle. Employees are not exempt from these laws.

9. Summary of Responsibilities

Supervisors

- Counsel employees and monitor their use of IT resources to ensure those resources are being used appropriately.

- Immediately notify the servicing Employee Relations Specialist when they are made aware of potential misuse of Government IT resources.

Employee Relations Specialists

- Determine whether misuse is indicated based on appropriate law, rule, regulation, or agency policy.

- Conduct an inquiry/investigation into the extent of the misuse of IT resource(s).

- Provide advice and guidance on appropriate disciplinary action.

Employees

- Ensure that personal use of IT resources is limited to personal time, does not interfere with official business, and involves minimal additional expense to the Government.

- Notify their immediate supervisor if they have reason to believe IT resources are being used for other than authorized purposes.

10. Glossary

C.F.R. Code of Federal Regulations.

Information Technology. The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the

Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others.

Information Technology (IT) Resources. Computers, computer peripherals, hardware, software, printers, cellular and land-line telephone equipment and services, copiers and facsimile machines, electronic mail, and the Internet, owned, leased, or otherwise in the possession of the REE agencies.

Investigation. A formal examination and evaluation of relevant facts to determine whether misconduct has taken place or, if misconduct has already been confirmed, to assess its extent and determine appropriate action.

Minimal Additional Expense. An employee's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services, and the employee's use of such equipment or services will not result in any additional expense to the Government, or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper.

Personal Use. Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

-Sd-

W.G. HORNER
Deputy Administrator
Administrative and Financial Management

United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

DEC 12 2008

TO: Agency Chief Information Officers

FROM: Charles R. Christopherson, Jr.
Chief Financial Officer
Chief Information Officer

SUBJECT: Use of USB Drives on USDA Systems

This memorandum reminds you of current USDA policy on Universal Serial Bus (USB) Drives. USB drives, sometimes known as thumb drives, while convenient for carrying large amounts of information, have several risks that need to be addressed. First, such drives are a possible way to infect Department systems with malware. USB drives are easily lost and stolen because of their size and portability. USB drives also allow malicious users with physical access to inconspicuously copy and steal entire hard drives of possibly sensitive information.

Currently USDA Departmental Manual, 3550-003 "Portable Electronic Devices and Wireless Technology" requires a formal risk assessment and agencies must plan and execute measures to safeguard systems and lower security risks to a manageable level. Additionally, USDA Policy requires all USDA portable electronic devices be encrypted.

On November 4, 2008, the United States Computer Emergency Readiness Team (US-CERT) released a Situational Awareness Report recommending that agencies ensure the following to help mitigate the risks of using USB drives:

- Password protect and encrypt USB drives.
- Lock USB ports or control the use of USB ports using configuration control software.
- Keep personal and business USB drives separate. Do not use personal USB drives on computers owned by your agency and do not plug USB drives containing government information into a personal computer.
- Keep systems up-to-date with the latest patches and anti-virus signatures.
- Do not plug an unknown USB drive into a computer. If a USB drive is found, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into a computer to view the contents or to try to identify the owner.

We have a core responsibility to ensure the security of all Department of Agriculture applications, systems, and the data inherent to those systems. If you have any questions about these procedures, please feel free to contact me.

USDA

United States Department of Agriculture

Research, Education, and Economics
Agricultural Research Service

JUN 15 2009

SUBJECT: Use of USB Drives on ARS Systems

TO: Deputy Area Directors
Area Information Technology Specialists

FROM: Domi Sanchez
Chief Information Security Officer

On December 12, 2008, the USDA CIO released a memorandum titled "Use of USB Drives on USDA Systems." This memo, along with the following documents, addresses the inherent risks and responsibilities involved with the use of USB thumb (flash) drives in Government computers.

- USDA Departmental Regulation (DR) 3180-001 Information Technology Network Standards (Appendix O) Section 16.0, states "Portable and mobile devices used to access the USDA network must be authorized, documented, and monitored. All data on such devices must be encrypted using FIPS 140-2 validated encryption unless the data has been determined to be non-sensitive, in writing, by the system owner and validated by USDA's Office of the Chief Information Officer (OCIO).

- USDA Departmental Manual 3550-003 states, "Strong encryption and authentication techniques will be used in the transmission and storage of sensitive information, where applicable. Each agency will secure and be accountable for PEDs (Portable Electronic Devices) including establishing password protection to devices, if available, and any built-in or removable flash memory used in such devices."

- United States Computer Emergency Readiness Team (US-CERT) released a Situational Awareness Report (SAR-08-309-01) recommending Agencies use passwords and encryption on USB drives to protect the contact information of personnel involved with Continuity of Operations and Disaster Recovery procedures.

ars

Office of the Chief Information Officer
Cybersecurity Staff
5601 Sunnyside Avenue • Beltsville, MD 20705-5143

To comply with these directives, all USB flash (thumb) drives used to store and/or transport ARS information must meet the following criteria:

- The USB drive's encryption module must be validated with the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard (FIPS) 140-2 encryption standard.

- The USB drive must not require Administrator rights or application installation to the desktop or laptop.

- The USB drive must lockdown, reformat, or auto-wipe after 10 or less intrusion attempts.

- The USB drive must not autonomously poll the Internet for updates to its drivers.

These actions are necessary to reduce the risk inherent in using USB drives.

ARS OCIO is currently evaluating a number of FIPS 140-2 NIST validated USB drives and will provide all Area IT Specialists the list of recommended products by July 31, 2009.

Regarding the use of USB drives, personal and business information must be kept on separate USB drives. Do not use personal or unknown USB drives on ARS computers and do not plug USB drives containing government information into a personally owned computer. If a USB drive is found, it should be given to your local IT security personnel or local IT Specialist.

If you have any questions regarding this USB flash (thumb) drive requirement, please contact Domi Sanchez at ARS-OCIO-CyberSecurity@ars.usda.gov.

cc:
Administrator's Council

USDA

United States Department of Agriculture

Research, Education, and Economics
Agricultural Research Service

May 20, 2009

SUBJECT: Use of Personally-Owned Equipment for Official Government Business

TO: Deputy Area Directors
Area Information Technology Specialists

FROM: Melinda L. McClanahan *Melinda L. McClanahan*
Chief Information Officer

In January 2009 USDA directed all agencies to disable the Outlook Web Access (OWA). Since then, my office has received several inquiries regarding the use of personally-owned equipment to conduct official Government business.

Department Regulation (DR) 3180-001, Information Technology Network Standards, September 30, 2008, states, "The USDA prohibits the use of personally owned information systems to directly access government networks for official U.S. Government business involving the processing, storage, or transmission of federal information. Personally owned information systems can be used to interface with government web interfaces designed to accommodate communication of specific information (e.g., Employee Personal Page and Outlook Web Access)." Guidance further states, "Exceptions to this policy will be considered only in terms of implementation time." ARS fully supports this directive, which can be found at http://www.ocio.usda.gov/directives/doc/DR3180-001.pdf.

OCIO acknowledges that some Areas have fully implemented this directive while others have achieved partial implementation. OCIO would like to collaborate with the DADs to develop a plan to phase in full implementation of the directive across the Agency. I have asked Domi Sanchez, Chief Information Security Officer, to take the lead in working with you on this effort.

The effort involves two tasks: 1) identifying those employees that are utilizing personally-owned equipment by means of VPN access to conduct ARS business and 2) replacing this equipment with government-owned equipment. OCIO understands that replacing equipment may be cost prohibitive and, therefore, a reasonable phased approached is needed that coordinates implementation with budget cycles and ARMP plans. I also encourage you to consider the distribution of any unused or surplus ARS desktops and laptops to replace personally-owned equipment used to conduct ARS business. The ARS equipment will need a VPN account and must be in accordance with Personal Property regulations and Cybersecurity rules and guidelines.

Domi will be contacting you soon to solicit your help in developing a plan. In the interim, each Area should enforce the directive in accordance with its current business needs and restraints as determined by Area senior management. The DADs are encouraged to work closely with their AITSs on these policies. If you have any questions, please contact Domi at ARS-OCIO-Cybersecurity@ars.usda.gov.

ars

Office of the Chief Information Officer
5601 Sunnyside Avenue • Beltsville, MD 20705-5119

USDA Websense Content Filtering
URL Exception Request Approval Process
ARS, OCIO, Cybersecurity
February 24, 2009

Websense Description:

The USDA network utilizes the Websense content filtering product to prevent employees from going to specific websites. These prohibited sites primarily contain material or information related to gambling, pornography, weapons, terrorist activities, etc.

The Department recently implemented more stringent filtering criteria and is now blocking certain types of advertisements from popping up or displaying on legitimate web sites. These advertisement sites have been blocked based on a recommendation from a US-CERT Situational Awareness Report regarding the possible presence of a computer worm located within the advertisement.

Users should still be able to view the information on the site, but advertisements may be blocked out or display USDA warning information. This does not mean that the user has clicked on a prohibited site, but that USDA is blocking the advertisement material.

URL Exception Request Approval Process:

1. If an employee attempts to access a site that has been blocked by the Department's web content filtering system, the USDA Change Management, Exception Request for the URL Filtering System form will pop up on the screen.

2. The employee should fill out all the requested fields, including the 'Technical Details' and the 'Business Justification' and click on the submit button.

3. A second form, the USDA URL Exception Request Approval Form, will then pop up containing the information the user entered on the previous screen. The user should print this form, sign, date, and fax it to 301-504-1034 to the attention of ARS, OCIO, Cybersecurity.

4. The ARS Information System Security Program Manager (ISSPM) will review the approval request and may contact the employee for additional information. If the ISSPM finds that the Agency has a legitimate business case for access to this site, the ISSPM and the Agency Chief Information Officer will sign the form and fax it to the Department. If the request is not approved, the ISSPM will contact the requestor with specific details.

This process usually takes approximately 2 to 3 business days. Questions regarding this process should be sent to ARS-OCIO-Cybersecurity@ars.usda.gov.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Situational Awareness Report- SAR-08-309-01

November 4, 2008

Using Caution With USB Drives

Overview

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks. USB drives have several inherent vulnerabilities due to the fact that they are unmanaged storage devices. US-CERT is issuing this document to inform agencies of the risks associated with USB drives as well as recommendations to protect against these risks.

What security risks are associated with USB drives?

USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable; therefore, making them popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use a USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on the system.

Attackers may also use USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including

passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives is that they can be easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. If the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

Recommendations

US-CERT recommends that agencies apply the following to help mitigate the risks of using USB drives:

- **Take advantage of security features** - Use passwords and encryption on USB drives to protect the data, and ensure the information on the drive is backed up in case it is lost.
- **Lock USB ports or control the use of USB ports using configuration control software.**
- **Keep personal and business USB drives separate** - Do not use personal USB drives on computers owned by your agency, and do not plug USB drives containing government information into a personal computer.
- **Keep systems up-to-date with the latest patches and anti-virus signatures.**
- **Do not plug an unknown USB drive into a computer** - If a USB drive is found, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into a computer to view the contents or to try to identify the owner.

US-CERT also recommends that agencies review the following documents available on the US-CERT website (http://www.us-cert.gov):

- Cyber Security Tip ST04-017 - Protecting Portable Devices: Physical Security
- Cyber Security Tip ST04-020 - Protecting Portable Devices: Data Security

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/

Document FAQ

What is a SAR? A Situational Awareness Report (SAR) is intended to provide warning of new security vulnerabilities, cyber incidents, and malicious code that is seen against or poses a threat to federal and state government networks or country CERT that US-CERT collaborates with.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

USDA

United States Department of Agriculture

Research, Education, and Economics
Agricultural Research Service

June 8, 2006

SUBJECT: Unauthorized Peer-to-Peer (P2P) Programs on Government Computers

TO: All Agency Employees

FROM: Melinda L. McClanahan /s/
Chief Information Officer

This memo is a reminder to all ARS Employees that the use of P2P software is prohibited on all USDA equipment and networks. In accordance with Office of Management and Budget Memo 04-06 on File Sharing Technology, "Federal computer systems or networks (as well as those operated by Contractors on the government's behalf) must not be used for the downloading of illegal and/or unauthorized copyrighted content." USDA does not consider "Limited Personal Use Policy" defined in DR 3300-1 or ARS P&P 253.4 as justification for downloading P2P or other programs that perform those functions.

P2P is a protocol often used to obtain freeware, shareware, and bootleg software. P2P exchange is made practical through web sites that act as clearinghouses listing people who have or want something. Some P2P applications allow computer users to directly access files from another hard drive such as, music (mp3), movies, and documents. Other types of P2P applications include gaming, telephony, and instant messaging.

The following list gives examples of some P2P software divided by category.

Instant Messaging /Telephony

- Yahoo Messenger
- Windows Messenger
- Skype
- MSN Messenger
- AOL Instant Messenger

ars

Office of the Chief Information Officer
5601 Sunnyside Avenue • Beltsville, MD 20705-5143
An Equal Opportunity Employer

File Sharing

- Bit Torrent
- Gnutelle
- Kazaa
- WinMX
- Napster
- PC Anywhere
- Edonkey
- Morpheus
- EMule
- Limewire
- BearShare
- Timbuktu

Instant Messaging/Telephony allows users to chat via text messaging in real time in addition to sharing files and initiating telephone calls over the Internet. File Sharing and gaming allows users to search each other's hard drives for specific files or information.

P2P file sharing can potentially compromise computer systems. The use of this software creates vulnerabilities which can be exploited by providing a means of introducing malicious code and other illegal material into a Government network. In addition, the software can allow inadvertent sharing of files by vulnerabilities or misconfiguration of the software.

To enforce Department Manual 3525-002 "Internet Use & Copyright Restrictions," USDA Cyber Security is monitoring all USDA networks for P2P traffic. Upon detection of this traffic, the ARS, OCIO, Cybersecurity Branch will be notified via the Incident Handling Process.

Having this software installed and/or running on Government equipment or networks is prohibited and appropriate disciplinary action will be taken. If you currently have this type of software installed on your government equipment, it must be removed. Should you require assistance to remove this software, please contact your local help desk.

If an exception to this policy is required, please prepare and send a valid business need to include your immediate supervisor's approval and signature and email your request to ARS-OCIO-Cybersecurity@ars.usda.gov.